



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/543,750	04/05/2000	Xavier Serret-Avila	7451.0020-00	6357

22852 7590 05/12/2004

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER

BROWN, CHRISTOPHER J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 05/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

3

20

Office Action Summary	Application No. 09/543,750	Applicant(s) SERRET-AVILA, XAVIER	
	Examiner Christopher J Brown	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 March 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-74 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 3-15, 31-35, 55-68 and 71-74 is/are allowed.
- 6) ☒ Claim(s) 1, 2, 16-25, 27-30, 36-44, 46, 48-52, 54, 69, 70 is/are rejected.
- 7) ☒ Claim(s) 26, 45, 47 and 53 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 April 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>5, 6, 7</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Objections

1. Claim 31 is objected to because of the following informalities: Step "l" appears to be mislabeled; it should be step "j". Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 65 recites the limitation "second stored check value" in line 1. There is insufficient antecedent basis for this limitation in the claim. This rejection could be overcome by rewriting claim 65 to depend on claim 64, rather than claim 1.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claim 1-2, 16, 28, 29, 36, 43, 46, 48, 49, 50, 52, 54, 69, 70 rejected under 35 U.S.C. 103(a) as being unpatentable over Gennaro US 6,009,176 in view of Fraser US 5,835,595 in view of Schneier "Applied Cryptography".

As per claim 1, Gennaro discloses generating a progression of check values (hashes), (Col 8 lines 25-40). Gennaro disclose inserting public key, size in bytes of the next

Art Unit: 2134

block, check value, and signature in the streaming data blocks, (Col 8 lines 30-40).

Gennaro discloses transmitting an electronic file and the progression of check values to a user's system via a data stream, (Col 8 lines 12-17, lines 30-37). Gennaro discloses receiving and authenticating of the data stream before the entire file is received, (Col 2 lines 35-42) Gennaro discloses including receiving the root check value (first block hash), and using the value and check values to authenticate portions of the data stream before the entire file is received, (Col 8 lines 57-67, Col 10 lines 20-50).

Gennaro does not disclose encryption. Gennaro does not disclose that each check value in the progression is derived from at least one other check value in the progression and from a hash of a portion of the electronic file.

Fraser discloses encryption and decryption of streaming data, (Col 2 lines 37-40). Fraser in combination with Gennaro, discloses encrypting and decrypting a root check value. It would be obvious to one skilled in the art to modify Gennaro's system with encryption to make it more secure over such insecure transfer mediums as the internet.

Schneier discloses N-hash function (page 433 Applied Cryptography). N-hash generates check values (hashes) with each check value (hash) being derived from at least one other check value in the progression and from a hash of a portion of the electronic file.

It would be obvious to one of ordinary skill in the art to modify the Gennaro-Fraser system with the N-hash of Schneier because it creates an authentication chain in the streaming file which increases security.

Art Unit: 2134

As per claims 18, 38, 41 Gennaro-Fraser-Schneier discloses the transformed portion of the file comprises a hashed portion of the file, (Schneier, page 433).

As per claim 19, Gennaro-Fraser-Schneier inserting a plurality of hashes in the file, each hash being inserted in proximity to a portion of the file to which it corresponds, (Gennaro Col 8 lines 25-40).

As per claim 20, 39, Gennaro-Fraser-Schneier discloses performing Md5 hashing on a first data block. Gennaro-Fraser-Schneier discloses N-hash operations to obtain further check values. Gennaro-Fraser-Schneier discloses signing the check values, (Gennaro Col 8 line 38). Gennaro-Fraser-Schneier discloses sending the data stream, it is inherent that it would be stored on a computer readable storage device.

As per claim 21, 30 Gennaro-Fraser-Schneier discloses a software hardware system with a 1.8 M bit buffer, it would be obvious on a PC system to use a hard drive, (Gennaro Col 5 lines 15-21).

As per claims 22, and 23, 51 Gennaro-Fraser-Schneier discloses that the first operation is a MD5 hash, (Gennaro Col 8 line 59).

As per claim 25, Gennaro-Fraser-Schneier disclose an input to the N-hash is a pre-defined data pattern (Schneier 433).

As per claim 27 Gennaro-Fraser-Schneier discloses the content includes multimedia data, (Gennaro Col 8 line 16).

As per claim 37, Gennaro-Fraser-Schneier discloses code for unsigned the digital signature, (Gennaro Col 8 lines 40-45).

Art Unit: 2134

As per claim 40 Gennaro-Fraser-Schneier discloses use of the data if more than a set number of portions has passed.

As per claim 42, Gennaro-Fraser-Schneier discloses MPEG video which would be inherently displayed in a screen, (Gennaro Col 8 line16).

As per claim 44 Gennaro-Fraser-Schneier discloses an error condition where an error is detected, (Gennaro Col 10 line 47).

Claims 26, 45, 47, and 53 are objected to due to their dependence on rejected independent claims.

Allowable Subject Matter

4. Claims 3 and 4-13, 14-15, 31-35, 55-68, 71-74 are allowed.

Conclusion


5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J Brown whose telephone number is 703-305-8023. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703-308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J. Brown


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100